

1999P1778

METHOD AND DEVICE FOR SECURING A MULTI-DimensionALLY
CONSTRUCTED CHIP STACK AND CHIP CONFIGURATION

5

Cross-Reference to Related Application:

This application is a continuation of copending International Application No. PCT/EP00/03834, filed April 27, 2000, which designated the United States.

Background of the Invention:

Field of the Invention:

The invention relates to a method and a device for securing a multi-dimensionally constructed chip stack, which has a plurality of part chips connected to one another at respective contact areas. At least one of the part chips includes appropriate functional components.

In this case, functional components are to be understood as
20 micro-electronic circuits or micro-mechanical components of any type integrated into the part chips. A chip can be understood to be, for example, a wafer or a part of a wafer made of a semiconductor material or another suitable material.

25 The problem on which the present invention is based is to ensure, in such a chip stack, that the connection between the

individual part chips at the respective contact areas cannot be undone or detached without such a damage being detected by an appropriate functional component. If such a damage can be determined, appropriate counter measures can be taken which, for example, prevent further operation of one or more functional components.

Hitherto, little consideration has been given to the problem of securing a multi-dimensionally constructed chip stack, since three-dimensional chip connections are not yet in widespread use.

Summary of the Invention:

It is accordingly an object of the invention to provide a method and a device for securing a multi-dimensionally constructed chip stack which overcomes the above-mentioned disadvantages of the heretofore-known methods and devices of this general type and which are able to make physical attacks on critical security chips, such as smart cards or code cards, detectable. In particular, dividing the chip stack in order to make access to parts of the chip should be detectable.

With the foregoing and other objects in view there is provided, in accordance with the invention, a method of securing a multi-dimensionally constructed chip stack, the method includes the steps of:

The present invention is based on the idea of integrating a multi-dimensional meandering line into the chip composite, through which, continuously or at specific time intervals, electrical signals are transmitted from a first point to a second point. In the simplest case, if the signals arrive at the second point or arrive unchanged, it is possible to draw conclusions from this relating to the intactness of the signal path located between them. In relation to the respective part chip, vertical feed-through contacts or plated-through holes are used for the purpose of connecting planar conductor track patterns of different part chips and, in this way, to provide a signal path running through all the part chips mounted one above another.

This has the advantage that the integration of the security device according to the invention can be carried out within the context of conventional process steps, in particular metallization and through-hole plating.

According to the invention, a continuous electrical reference signal path running from the transmitting device to the receiving device is formed, and an electrical reference signal is transmitted over the path at the same time as the electrical signal is transmitted. This ensures that no

the respective contact areas, a device for securing the multi-dimensionally constructed chip stack, including:

conductor tracks provided in respective ones of the part
5 chips;

feed-through contacts provided at the respective contact areas, the feed-through contacts interconnecting the conductor tracks of different ones of the part chips such that a
10 continuous electrical signal path extending through the part chips is formed, the continuous electrical signal path having a first end and a second end;

a transmitting device provided at the first end of the
15 continuous electrical signal path;

a receiving device provided at the second end of the continuous electrical signal path, the receiving device being configured to receive an electrical signal transmitted via the
20 continuous electrical signal path;

a continuous electrical reference signal path extending from the transmitting device to the receiving device; and

25 a determining device operatively connected to the receiving device, the determining device determining that there is a

Brief Description of the Drawings:

Fig. 1 is a schematic illustration of a chip stack constructed from three part chips and having a security device according to a first exemplary embodiment of the invention;

5

Fig. 2 is a schematic illustration of a chip stack constructed from three part chips and having a security device according to a second exemplary embodiment of the invention;

0 Fig. 3 is a schematic illustration of a chip stack constructed from three part chips and having a security device according to a third exemplary embodiment of the invention;

5 Fig. 4 is a schematic illustration of a chip stack constructed from three part chips and having a security device according to a fourth exemplary embodiment of the invention;

20 Fig. 5 is a schematic illustration of a chip stack constructed from three part chips and having a security device according to a fifth exemplary embodiment of the invention; and

Fig. 6 is a schematic illustration of a chip stack constructed from three part chips and having a security device according to a sixth exemplary embodiment of the invention.

25

Description of the Preferred Embodiments:

Referring now to the figures of the drawings in detail and first, particularly, to Fig. 1 thereof, there is shown a schematic illustration of a chip stack constructed from three
5 part chips, having a securing device according to a first exemplary embodiment of the invention. In the figures, identical reference symbols designate identical or functionally identical elements. In Fig. 1, TC1, TC2, TC3 designate a first, second and third part chip which are
10 connected (for example soldered) to one another in the form of a stack at respective contact areas K12, K23. The respective part chips contain security-sensitive functional components which, for reasons of simplicity, are not illustrated in the figures.

15 LB1, LB2 and LB3 designate conductor tracks which are provided in the corresponding part chips TC1, TC2, TC3, which are created using known planar technology and, in the example shown, are buried under the respective surface of the relevant
20 part chip (for example under an insulating layer).

In order to connect the conductor tracks, feed-through contacts or plated-through holes V (vias with a conductive filling) through the part chips TC1, TC2, TC3 are provided,
25 which ensure that a continuous electrical signal path running through all the part chips is formed. Provided at a first end

of the electrical signal path is a transmitting device S, and a receiving device E is provided at a second end of the electrical signal path.

5 For securing the multi-dimensional chip stack constructed in this way, during operation an electrical signal is led from the transmitting device S to the receiving device E at regular intervals, for example in a one-second cycle. The receiving device contains an intelligent circuit or determining circuit, which is only schematically shown in Fig. 2 and which determines that there is damage to the chip stack if the electrical signal Si cannot be received in the receiving device E. This determining device further ensures that security-relevant functional components in the part chips TC1, TC2, TC3 are deactivated if damage to the chip stack is determined. For example, such deactivation may be the deletion of memory contents of memory components. The deactivation may be performed by a deactivation device which is schematically indicated in Fig. 2.

20

The type of electrical signal is substantially as desired. It needs only to be a pattern whose structure is known to the receiver.

25 The continuous signal path shown in Fig. 1 has the form of a
meander lying in a vertical plane. In order to extend the

5 (depth) .

20 artificial transmitting device can be used instead of the real
transmitting device S to confuse the receiving device E.

25 conductor tracks and feed-through contacts, and is shown here
only as a schematic line merely for reasons of simplification.

5

5

5

20

25

5 in the case of this embodiment, two-dimensional meandering conductor track patterns M1, M2 are incorporated into the signal path. These meandering conductor track patterns are provided on the upper and lower end faces of the chip stack and are used to protect these two large exposed end faces.

100

125

20

25

20 5

In particular, a solder metal can also be applied to one side of the lower chip, and the circuit can be projected on all sides in this way.

5 In the sixth embodiment shown, the transmitting device S and
the receiving device E are accommodated in the central part
chip. The signal path runs upward from the transmitting device
S into the meandering conductor track layer MM2, from there,
via the feed-through contacts V, into the meandering conductor
0 track layer MM1 and vertically upward from there to the
receiving device E.

Although the present invention has been described above using preferred exemplary embodiments, it is not restricted to these, but can be modified in manifold ways. In particular, the present invention is not restricted to three interconnected part chips, but can be used on any desired combination of part chips. In addition, the two-dimensional or three-dimensional configuration of the continuous signal path can be divided up as desired, corresponding to the geometric relationships of the individual chips.

The transmitting device and the receiving device can be located in one of the part chips, but can likewise be provided outside the chips, for example in a mount or clamping device for the chip.

5 can be added.